Република България
ИКОНОМИЧЕСКИ
И СОЦИАЛЕН СЪВЕТ

АНАЛИЗ

„Европейските изисквания и перспективи за киберустойчива България“

(разработен по собствена инициатива)

Април 2024 г.

В Плана за дейността на Икономическия и социален съвет за 2024 г. е включен за разработване по собствена инициатива анализ на тема: „Европейските изисквания и перспективи за киберустойчива България“.

Анализът бе разпределен на Комисията по европейски политики и европейски процес.

За докладчик по анализа беше определен Атанас Темелков – член на ИСС от група I.

Комисията проведе две заседания на 14.03. и 08.04.2024 г., като прие проекта на анализа.

На своята пленарна сесия, проведена на 17 април 2024 г., Икономическият и социален съвет прие настоящия анализ.

Настоящият информационно-аналитичен документ, е разработен в съответствие с Годишния план на Икономическия и социален съвет и има за цел да представи сложният контекст на политиката за киберсигурност на ЕС, да идентифицира основните перспективи и предизвикателства за ефективното осъществяване на тази политика в рамките на България. В него са обхванати приоритетно темите свързани с мрежовата и информационна сигурност. Анализът е основан на преглед и проверка на публично достъпната информация в официални документи, документи изразяващи позицията и проучвания на трети страни. В хода на изготвяното му бяха взети предвид актуална към 10.02.2024 г. информация в сферата на киберсигурността на европейско и национално ниво.

Докладът е с ограничения от поверителност на данните за заплахите, инциденти и по-специално мерките за реагиране, свързани със спецификата в дейностите по два от стълбовете на киберсигурността – киберпрестъпност и киберотбрана. Обменът на такава информация и технически аспекти, създава ненужен риск, свързан с идентифицирането и излагане на уязвимости на национална инфраструктура за сигурност.

ИЗВОДИ И ПРЕПОРЪКИ

Изводи:

1. В рамките на Европейския съюз (ЕС) в последните няколко години са разработени и приети редица правно-нормативни документи (3 регламента, 3 директиви,1 компендиум, 2 нструментариума, няколко съобщения и др.) регламентиращи изисквания към държавите членки на Съюза(ДЧ) за постигане на високо ниво на киберсигурност. Документите са за конкретни предметни области, както използваните подходи и терминология се различават, което създава не яснота и не еднозначност в прилагането им;

2. Не се установи систематичен подход в страната за информиране по новоприети в областта на киберсигурността в ЕС правно-нормативни документи и за предприетите във връзка с тях действия на национално ниво;

3. Актуализираната национална стратегия за киберсигурност „Киберустойчива България 2023“ е с изтекъл срок на приложимост;

4. Не се установи наличие на приета Пътна карта към актуализираната стратегия „Киберустойчива България 2023“;

5. Разработването на нова Национална стратегия за киберсигурност не е предвидено в Програмата за управление на правителството от юни 2023 г, до декември 2024 г. ;

6. Законът за киберсигурност транспонира напълно адекватно Директива ЕС 2016/2248, като надхвърля в някои случаи предвидените изисквания. Следва да се подчертае обаче, че съгласно **Директива (ЕС) 2022/2555 трябва** да бъде изменен и допълнен и приет от Народното събрание до 24 октомври 2024 г. Това предполага много добре организирани действия. Особено тясна координация е необходима между Министерство на електронното управление (МЕУ), Комисията за финансов надзор Министерство на финансите (МФ), Министерство на вътрешните работи (МВР) и др. При изготвянето на Закона за изменение и допълнение на Закона за киберсигурност следва да се вземат предвид освен Директива (ЕС) 2022/2555 и всички други релевантни на темата киберсигурност документи;

7. Дейността на Съвета по киберсигурност е спорадична и не достатъчно пълноценна. (Съветът е този който трябвало да предложи на Министерския съвет за приемане: Стратегия за киберсигурност на Министерския съвет до 31.12. 2023 г., Национален план за управление на киберкризи; начини за хармонизиране и

координиране на секторни политики за постигане на високо общо ниво на киберсигурност на икономиката и на обществото, и координиране и управление по време на дейностите на държавно ниво при мащабни киберинциденти, кризи и др.;

8. Националните компетентни органи и Екипите за реагиране при инциденти с компютърната сигурност, създадени с РМС № 192/09.2019 г., не разполагат съгласно изискванията на Закона за киберсигурност (чл.16, ал.13) с технически, финансови и човешки ресурси за да гарантират, че са в състояние да изпълняват ефективно възложените им задачи. Обезпечаването на органите по киберсигурност от съответните административни органи (Министерство на енергетиката, Министерство на регионалното развитие и благоустройството, Министерство на здравеопазването, Министерство на транспорта и съобщенията и МЕУ) с необходимия и изискуем по Закона за киберсигурност технически, финансов и административен ресурс е сериозен и непреодолим проблем за тях. В повечето функции, вменени на тези органи и екипи са възложени за изпълнение по съвместителство на ИТ служители;

9. По аналогичен начин стоят и въпросите с обезпечаването с технически, финансови и човешки ресурси на Националния орган за сертифициране на киберсигурността и Националния координационен център ситуирани с РМС в МЕУ.

10. Моделът за „Децентрализиран подход“, установен в стратегическата рамка за управление на киберсигурността в страната има своите особености.

Някои от тези особености са:

а)Системата за киберсигурност е с разпределена отговорност без ясно определено водещо и отговорно за цялостното състояние на киберсигурността ведомство;

б) Подходът изисква много тясно сътрудничество и координация между отговорните ведомства и прилагането на принципа за субсидиарност;

б) Предвидените в Закона за киберсигурност дейности по сътрудничество и координация следва да се осъществяват посредством Национална координационна и организационна мрежа и национален киберситуационен център. Същите не са изградени, поради което сътрудничеството и координацията не се извършват пълноценно;

в) Мрежата и Центъра служат за обмен на информация и координиране на действия, но нямат правомощия спрямо включените в нея ведомства;

г) МЕУ в качеството си на национален компетентен орган за административните органи, следва да извършва контрол на спазването на изискванията за мрежова и информационна сигурност и в самото министерство, което е явен конфликт на интереси.

11. МЕУ чрез дирекция „Мрежова и информационна сигурност“ (личен състав 22 бр.) изпълнява нормативно вменените му задължения като национален компетентен орган; национално единно звено за контакти; национален орган за сертифициране на киберсигурността (с две различни и независими едно от друг направления – сертифициране и надзор); Национален координационен център по киберсигурност. Следва да се има предвид, че с въвеждането на ДМИС 2 и произтичащите от това допълнителни изисквания за създаване на национална рамка за управление на мащабни киберинциденти и киберкризи налагат създаване (определяне) на национален компетентен орган за управление на киберкризи. Освен това Дирекцията трябва да разполага с капацитет, с който да подпомага министъра на електронното управление при провеждането на държавната политика; при извършването на контрол и проверки по спазване на изискванията за МИС в над 600 административни органа и над 5000 лица осъществяващи публични функции и организации предоставящи обществени услуги; по планиране, подготовка и провеждане на национални киберучения и др.

12. С приемането на Закона за изменение и допълнение на Закона за киберсигурност и въвеждането с него на нови субекти при сегашния модел на „Децентрализиран подход“, ще се наложи да се създадат минимум пет нови Национални компетентни органи и съответно Екипи за реагиране при инциденти в компютърната сигурност. На практика само в областта на МИС ще трябва да функционират в съответствие с изискванията на ДМИС 2, не по-малко от десет броя национални компетентни органи и десет екипи за реагиране при инциденти с компютърната сигурност към тях.

13. За създаването на условия за разрешаването на недостига с ресурси е необходимо преосмисляне на досегашния модел на Рамката за управление на киберсигурността в страната.

14. Не са установени публични документи, изискуеми по Закона за киберсигурност, определящи – нива на оценка на заплахата от кибератаки и

кибератаки и критерии за определянето им; степените за определяне нивото на готовност за противодействие на кибератаки и киберинциденти в зависимост от нивото на заплахата; мерките които се предприемат при съответните степени на готовност.

15.Органите по киберсигурност активно участват в повечето международни учения организирани по линия на ЕС и НАТО. Недооценен е въпроса с планиране, подготовка и провеждане на национални и секторни учения по киберсигурност. Последното национално учение е проведено през 2019 г.

16. В рамките на месеца на киберсигурността (провежда се ежегодно през м. Октомври) се организират различни, но некоординирани мероприятия за повишаване на киберсигурността , както от публични органи, така и от частни и неправителствени структури.

17. Не се установиха предприети действия от компетентните за това органи за прилагане на европейската квалификационна рамка в сферата на киберсигурността;

Препоръки :

1.С оглед на това, че е в ход процес на изготвяне на Закон за изменение допълнение на Закона за киберсигурност да се прецени целесъобразността от преминаване към модел на управление на системата за киберсигурност „Централизиран подход“.

Тук следва да се има предвид и преобладаващата практика в ДЧ, която е базирана на използването на модел „Централизиран подход“. Такива ДЧ са Германия, Франция, Италия, Испания, Чехия, Румъния, Нидерландия, Словакия и др.

2. При положително решение по предходната точка, промяната да се отрази своевременно в нормативните документи.

3. Да се предприемат мерки за изготвяне на Национална стратегия, която да е съобразена с изискванията заложени в Регламент (ЕС)2022/2554 и която логически следва да предхожда изготвянето на Закона за изменение и допълнение на Закона за киберсигурност. При разработване на Стратегията биха могли да се използват съществуващи възможност за проектно финансиране.

4. При изготвянето на Закона за изменение и допълнение на Закона за киберсигурност да се вземе предвид комплекта документи по киберсигурността,

приет от ЕС в края на 2022г., както и други релевантни документи в областта на киберсигурността.

5. В процеса на подготовка и провеждане на предстоящите избори на национално и на европейско ниво, да се използва специално подготвения за целта Компендиум от ЕС, включително да се планират, подготвят и провеждат таргетирани национални киберучения.

6. Да се предприемат мерки за постигане на съответствие с изискванията на Директива (ЕС) 2022/2555, Регламент (ЕС) 2019/881, Регламент (ЕС)2021/887 за гарантирано от ДЧ обезпечаване на съответните органи за киберсигурност с необходимите технически, административни и финансови ресурси, за да изпълняват ефективно и ефикасно задачите си.

7. Да се оптимизира дейността на Съвета по киберсигурността, с цел ефективно осъществяване на правомощията и функциите си.

8. Да се създаде и функционира механизъм за контрол на всички нива в системата за киберсигурност по отношение степента и качеството на изпълняваните задължения, в съответствие с изискванията на нормативните документи.

9. Да се предприемат от компетентните административни органи необходимите действия за прилагане на Европейската квалификационна рамка за умения в киберсигурността.

10. Да се използват пълноценно възможностите от участие в различни групи и формати в рамките на ЕС за активно отстояване на националните интереси в сферата на киберсигурност.

11. Да се предприемат необходимите действия (може би от МЕУ, като водещо по МИС) за систематичен подход по информиране за новоприети правно-нормативни документи на ниво ЕС в областта на киберсигурността и за необходимостта от предприемане на адекватни мерки и действия във връзка с тях на национално ниво.

I. УВОД

Информационните и комуникационните технологии и (ИКТ) са ключов фактор за икономическия растеж на държавите членки на Европейския съюз и на Съюза, като цяло са жизнено важен ресурс за националните стопанства. Те са съставен елемент в сложни механизми в комплексни системи които управляват и

осигуряват функционирането на структуроопределящи отрасли в икономиките ни, като енергетика, транспорт, съобщения и здравеопазване. В същото време редица бизнес модели са планирани и функционират при наличието на устойчиви интернет, достъп до него и безотказно функциониране на мрежите и информационните системи.

Безспорни са ползите от все по-растящия цифров свят, но на вниманието ни трябва да стоят и опасностите с които е съпроводен този процес. По данни от различни източници в последните години (особено след 2022 г.), броят на киберинцидентите в рамките на ЕС расте с тревожни темпове. В резултат на това може да се наруши функционирането на жизнено важни критични инфраструктури, на съществени услуги, като здравеопазване, електроенергийни и др.

Киберзаплахите могат да бъдат непреднамерени и преднамерени зад които стоят криминални, икономически, политически мотивирани, държавно спонсорирани лица и организации. В отделни случаи зад киберзаплахите стоят и цели държави. Непреднамерените заплахи пък могат да се дължат на човешки грешки, природни бедствия, технически проблеми и др..

Силно засегната е икономиката на Европейския съюз от престъпления и кибератаки в киберпространството насочени към както към публичния сектор, така и към частния сектор и отделни граждани. Анализите на регистрираните киберинциденти показва, че се използват все по-различни и сложни способи, включително и с използването на изкуствен интелект за кражба на данни, криптиране на налична информация и изнудване за откуп.

Спонсориран от отделни държави, икономическият шпионаж представлява също сериозна заплаха за държавите в европейското пространство.

В държави извън ЕС се наблюдават неправомерно използване на възможностите на киберпространството, за да се осъществява следене, наблюдаване и контрол над техните граждани. Един от приоритети на ЕС в тази насока е противодействие на тези действия, насърчавайки демократичните права и свободата на гражданите, като спомага за спазване на основните им права в цифрова среда.

Основните заплахи идентифицирани от Агенцията на ЕС за киберсигурност (ENISA), подредени по тяхната значимост за Съюза са:

рансъмуер (ransomware), зловреден код, заплахи за наличност, социално инженерство, заплахи срещу данни, атаки срещу веригите за доставки и др.

Броят и сложността на кибератаките и киберпрестъпността се увеличават в цяла Европа. Тази тенденция ще продължи да се засилва в бъдеще, тъй като до 2025 г. се очаква 41 милиарда устройства в световен мащаб да бъдат свързани с предметите свързани с интернет (IoT).

Всички тези фактори обясняват защо правителства на ДЧ разработват национални стратегии за киберсигурност и отделят повишено внимание на многобройните заплахи в киберпространство, като на важен фактор в международните отношения. Това налага ЕС, да предприеме адекватни пропорционални, технически, технологични и организационни мерки за постигане високо ниво на киберсигурността в Съюза.

II.ОСНОВНА ЧАСТ

II.1. Европейски изисквания за киберсигурност - Киберсигурността в дневния ред на ЕС

II.1.1 Приети от ЕС Правно-нормативни документи в сферата на киберсигурността

Съдържащите се в тази част на Анализа документи, са разгледани с фокус върху поставените от страна на ЕС изисквания в сферата на киберсигурността.

II.1.1.1 Стратегия на ЕС за киберсигурност

Стратегия на ЕС за киберсигурност за цифровото десетилетие

В края на 2020 г. беше представена Новата стратегия на ЕС за киберсигурност, от Европейската комисия и Европейската служба за външна дейност. За достигане на цифровото бъдеще на Европа, ключова роля се предвижда да има нова стратегия за киберсигурност.

Стратегията посочва начините и способите, с които ЕС ще постигне пълноценна защита от киберзаплахите на институциите на Съюза и на гражданите от ДЧ. Посочени са пътищата за участие на Съюза в международното сътрудничество в тази сфера и как той да има водеща роля за осигуряването на устойчив интернет.

В рамките на предходни стратегии се отчита, че е постигнат напредък, въз основа на който настоящата стратегия представя конкретни предложения за задействане на три основни инструмента — регулаторен, инвестиционен и

политически — засягащи три области на действие на ЕС — (1) устойчивост, технологичен суверенитет и лидерство, (2) изграждане на оперативен капацитет за предотвратяване, възпиране и реагиране и (3) постигане на напредък в създаването на световно и отворено киберпространство.

Инвестициите в цифровата сфера следва да включват като задължителен компонент киберсигурността. Това ще допринесе за стимулиране европейския пазар за киберсигурност.

Горепосочените основни положения са обективирани в Стратегията в следните три направления и в дейностите към тях:

Първо направление - Устойчива инфраструктура и услуги от критично значение.

Основни акценти - В основата на единния пазар за киберсигурност са заложени правилата на ЕС относно мрежовата и информационната сигурност (МИС). Комисията предлага реформа на тези правила при преразглеждането на Директивата за МИС(2016/1148), за да се повиши киберустойчивостта на всички значими публични и частни сектори, които изпълняват важна функция за икономиката и обществото; осигуряване на устойчива инфраструктура и услуги от критично значение, създаване на европейски Кибер щит (Мрежа от оперативни центрове за сигурност), подкрепа за малки и средни предприятия чрез иновационни центрове; свръхсигурна комуникационна инфраструктура (правителствени спътникови електронни съобщения, сигурна квантова комуникационна инфраструктура); осигуряване на широколентови мобилни мрежи от следващо поколение; сигурност на предметите свързани с интернет(IoT); по-голяма сигурност на Интернет в глобален мащаб; засилено присъствие във веригите за доставки на технологии, полагане на усилия за повишаване квалификацията на европейската работна сила в информационното пространство; в сферата на образованието усилията да се насочват към повишаване на уменията.

Второ направление – *Изграждане на оперативен капацитет за предотвратяване, възпиране и реагиране*

Основни акценти – съвместни звена за киберсигурност(част от европейска рамка за управление на киберкризи); борба с киберпрестъпленията; създаване на инструментариум за кибердипломация на ЕС - създаване на работна група за киберразузнаване в рамките на центъра за анализ на информацията, допълнителни

мерки и хоризонтални санкции в инструментариума за кибердипломация, сътрудничество с НАТО); укрепване способностите за киберотбрана, преглед на Политическата рамка на ЕС за киберотбрана, постоянно структурирано сътрудничество, План за действия на Комисията относно полезните взаимодействия между гражданската, отбранителната и космическата промишленост;

Трето направление - Постигане на напредък в създаването на световно и отворено киберпространство

Основни акценти – водеща роля на ЕС по отношение на стандартизацията, в международен план (засилване на процеса на стандартизация в международен план), насърчаване отговорното поведение на държавите в киберпространството, (конвенцията от Будапеща за престъпления в киберпространството); сътрудничество с партньорите и общността от заинтересовани страни; укрепване на световния капацитет с цел повишаване на устойчивостта в световен мащаб.

Предмет на стратегията са и въпроси по киберсигурността, отнасящи се до институциите, органите и агенциите на ЕС.

За дейностите по всяко едно от гореизложените направления, в Стратегията са посочени за постигане съответни стратегически цели.

II.1.1.2 Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета от 17 април 2019 година относно Агенцията на Европейския съюз за киберсигурност (ENISA) и сертифицирането на киберсигурността на информационните и комуникационните технологии.

С Акта на ЕС за киберсигурността приет през 2919 г. се дава отговор на въпрос какво точно представлява киберсигурността, като се дава ясно и единно за рамките на Съюза определение.

Наред с това Актът на ЕС за киберсигурността въвежда:

а) Нов и по-засилен мандат за Агенцията на ЕС за киберсигурност (ENISA)

б) Рамка за сертифициране на киберсигурността.

<u>Нов мандат на ENISA</u>

Агенция на ЕС за киберсигурност се основава на структурите на своя предшественик – Агенцията на Европейския съюз за мрежова и информационна сигурност, но със засилена роля и постоянен мандат.

Агенцията има за цел да оказва помощ на ДЧ, институциите на ЕС и други заинтересовани страни в борбата с кибератаките. ENISA е орган на ЕС, който има за задача да осигури високо равнище на киберсигурност в Европа. С Акта се предоставя постоянен мандат на Агенцията, предоставят се допълнителни ресурси и нови задачи. ENISA ще има водеща роля в създаването и поддържането на европейската рамка за сертифициране на киберсигурността, като подготви техническата основа за европейските схеми за сертифициране.

ENISA има мандат да оптимизира сътрудничеството на оперативно ниво в рамките на ЕС, като помага на ДЧ, да се справят с киберинциденти в случаи на необходимост, и подпомага координацията на ЕС при широкомащабни трансгранични кибератаки и киберкризи.

ENISA е предвидено да изпълнява ролята на секретариат на европейската мрежа от национални екипи за реагиране при инциденти с компютърната сигурност (CSIRT), създадена с Директивата относно сигурността на мрежите и информационните системи (Директивата за МИС).

<u>Рамка за сертифициране на киберсигурността</u>

Рамката за създаването на европейски схеми за сертифициране на киберсигурността има за цели: да се гарантира подходящо ниво на киберсигурност за ИКТ продукти, ИКТ услуги и ИКТ процеси в Съюза: - да се избегне разпокъсаност на вътрешния пазар по отношение на схемите за сертифициране на киберсигурността в Съюза; да се подобрят условията за функционирането на вътрешния пазар.

До приемането на Акта не съществува общоевропейски документ уреждащ дейностите в тази сфера, което е предпоставка за все по-голям риск от разпокъсаност и пречки между ДЧ за комуникация.

Основни акценти

Непрекъсната работна програма на Съюза за европейското сертифициране на киберсигурността – ЕК набелязва стратегическите приоритети за бъдещите европейски схеми за сертифициране на киберсигурността – включва списък на ИКТ продукти, процеси и услуги субект на стандартизацията; наличието и разработването на национални схеми за сертифициране; развитие на картата на киберсигурността, пазарно търсене и др.

С Регламента се установяват ред за изготвяне, приемане и преразглеждане на европейски схеми за сертифициране на киберсигурността.

Предвижда се схемите да бъдат проектирани така, че да бъдат постигнати посочените в Регламента цели – опазване на информацията/данните в процеса на сертифициране; сертифициращите органи да имат достъп само до необходимото им; да се установят и документират известните зависимости и уязвимости да се регистрира до кои данни, услуги или функции е бил осъществен достъп; да се провери субекта за сертифициране дали не съдържа известни уязвимости; ограничаване на достъп до информация/данни в случай на инциденти и др.

По-специално, всяка европейска схема следва да посочва: обхванатите категории продукти и услуги; изискванията за киберсигурност, като например стандарти или технически спецификации; вида на оценката, като например самооценка или трета страна; планираното ниво на увереност и др.

Нива на увереност на европейските схеми за сертифициране на киберсигурността

В Акта са предвидени следните нива на увереност за ИКТ продукти, ИКТ процеси и услуги „базово“, „съществено“ или „високо“. Нивото на увереност следва да е съизмеримо със степента на риска, свързан с предвидената употреба на ИКТ продукта, ИКТ процеса или ИКТ услугата, с оглед на вероятността от инцидент и неговото въздействие. Сертификати за киберсигурност и ЕС декларациите за съответствие посочват всяко ниво на увереност, предвидено в европейска схема за сертифициране на киберсигурността.

1. ниво на увереност „базово“, дава увереност, че ИКТ продуктите, ИКТ услугите и ИКТ процесите, за които този сертификат или тази ЕС декларация за съответствие са издадени, отговарят на съответните изисквания за сигурност, включително функционалности за сигурност, и че са били оценени на ниво, което има за цел да се сведат до минимум известните основни рискове от инциденти и кибератаки.

2. ниво на увереност „съществено“, дава увереност, че ИКТ продуктите, ИКТ услугите и ИКТ процесите, за които този сертификат е издаден, отговарят на съответните изисквания за сигурност, включително функционалности за сигурността и, че са били оценени на ниво, което има за цел да се сведат до минимум известните киберрискове, рискове от инциденти и кибератаки, извършвани от субекти с ограничени умения и ресурси.

3. ниво на увереност „високо“ дава увереност, че ИКТ продуктите, ИКТ услугите и ИКТ процесите, за които сертификатът е издаден, отговарят на съответните изисквания за сигурност, включително функционалности за сигурност, и че са били оценени на ниво, което има за цел да се сведе до минимум рискът от най-висш тип кибератаки, извършвани от субекти със значителни умения и ресурси.

Предвидена е възможност да се извършва самооценяване на съответствието, като отговорност за нея носи единствено производителят или доставчикът.

Актът предвижда сертифицирането да бъде доброволно. За ниво на увереност „високо“, европейският сертификат за киберсигурност може да бъде издаден само от национален орган за сертифициране на киберсигурността и по изключение - от орган за оценяване на съответствието .Предвидено е също така, сертификата да важи за определен период от време и е валиден във всяка ДЧ.

Актът предвижда ДЧ да не въвеждат нови национални схеми за сертифициране на киберсигурността на ИКТ продукти, ИКТ услуги и ИКТ процеси за вече обхванати от европейска схема за сертифициране.

Всяка ДЧ може да създаде един или повече такива органи, които трябва да разполагат с достатъчно ресурси за упражняване на правомощията си и за изпълнение на възложените им задачи по ефективен и ефикасен начин. За Националният орган са предвидени девет функции свързани с надзора и изискване да притежава не по-малко от подробно посочени правомощия. Националният орган за сертифициране е независим от субектите, върху които упражнява надзор, по отношение на своята организация, решения за финансиране, правна структура и процес на вземане на решения. В рамките на Националния орган за сертифициране следва да има гарантирано разграничение на дейностите по сертифициране и на тези по надзора.

В Акта е предвидено извършване на партньорски проверки – от най-малко два национални органа за сертифициране на киберсигурността от други ДЧ, по пет критерия, най-малкото веднъж на пет година.

II.1.1.3 Регламент (ЕС) 2021/887 на Европейския парламент и на Съвета от 20 май 2021 година за създаване на Европейски център за промишлени, технологични и изследователски експертни познания в

областта на киберсигурността и на мрежа от национални координационни центрове

С Регламента, ЕС предвижда да се създаде Европейска мрежа и Експертен център за киберсигурност. Всяка ДЧ, определя един национален координационен център, който ще бъде звено за контакт на национално равнище за експертната общност и Експертния център. На европейско ниво те ще се обединят в Мрежа от национални координационни центрове.

Създава се и експертна общност в областта на киберсигурността, която включва голяма, отворена и разнообразна група от участници в технологиите за киберсигурност.

Като резултат от влизането в сила на Регламента, научноизследователските и технологични общности и публични органи ще получат достъп до ключови способности - съоръжения за изпитване и експериментиране; принос за преодоляване на недостига на умения, като осигури достъп на най-добрите таланти до широкомащабни европейски проекти за научни изследвания и иновации в областта на киберсигурността.

Основни акценти:

. Мисията на Експертния център е да помага на Съюза в три направления - да укрепи лидерството и стратегическа активност в сферата на киберсигурността; да подкрепя технологичния капацитет на Съюза; да увеличи конкурентоспособността на промишлеността си в световен мащаб; да използва осигурените финансови ресурси по Програми „Хоризонт Европа“ и „Цифрова Европа“.

Цели на Експертния център:

1.обща цел насърчава научни изследвания, иновациите и внедряването в сферата на киберсигурността;

2. специфични цели – утвърждава киберустойчивостта; допринася за изграждане на европейска екосистема за киберсигурност; в интерес на публичния сектор, промишлеността, гражданското общество да увеличава способностите и знанията в сферата на киберсигурността.

Задачи за изпълнение от Европейския център

За постигане на тези си цели, Европейският център се предвижда да изпълнява стратегически задачи по изпълнението:

1.в разработването на Програма, установяване на приоритети за Центъра, работа по увеличаване на промишлени и технологичен капацитет, внедряване на продукти за киберсигурност; оказване помощ на малки и средни предприятия; експертни съвети и консултации и др.

2. координиране работата на Мрежата; подготовка на Годишна програма оказване помощ за „Усъвършенстване на цифрови умения“ и др.

Национални координационни центрове

Центърът е субект от публичния сектор или субект по-голямата част от които се притежава от държавата.

Към Националният координационен център е предвидено изискване да може изпълнява определени задачи (10 на брой), свързани преди всичко с предоставяне на експертен опит; поощряване на гражданското общество за участие на национално равнище в трансгранични проекти; оказване техническа помощ на заинтересовани лица на фаза „кандидатстване“; да взаимодействат с национални органи по отношение на принос към за разпространение на образователни програми; да популяризират дейности инициирани от Европейския център допустими за участници на национално ниво

Експертна общност в сферата на киберсигурността

Общността допринася за осъществяване на мисията на Експертния център и на Мрежата. Състои се от промишлеността, академични и научноизследователски организации, асоциации на гражданското общество. Членове на Общността могат да бъдат само субекти, които са установени на територията на ДЧ от области – академични среди, обучение и образование, промишлени разработчици, мрежова и информационна сигурност, етика, стандартизация и сертификация.

Финансово участие на Съюза и на ДЧ

Експертният център се финансира от Съюза, а съвместните действия се финансират от Съюза и с доброволни вноски от ДЧ. Съюзът покрива административните и оперативните разходи на Експертния център -
до 1 649 566 000 EUR от програмата „Цифрова Европа“. Посочени са и други източници за финансиране на преди всичко административни дейности.

Експертният център изпълнява действията в областта на киберсигурността по програма „Цифрова Европа“ и програма „Хоризонт Европа“. ДЧ доброволно участват в съвместни действия чрез свои доброволни финансови вноски и/или непарични вноски. Ако ДЧ участва в съвместно действие, финансовата вноска на тази ДЧ членка покрива административните разходи пропорционално на нейната вноска за съвместното действие. Административните разходи за съвместни действия се покриват чрез финансови вноски. Вноските от всяка ДЧ могат да бъдат под формата на подкрепа от тази ДЧ, предоставена в рамките на съвместно действие на бенефициерите, установени във въпросната ДЧ. Непаричните вноски на ДЧ се състоят от допустимите разходи, направени от националните координационни центрове и други публични субекти, когато участват в проекти, финансирани по настоящия регламент, като се приспадне участието на Съюза в тези разходи. Регламентът разглежда и др. финансови въпроси относими към ДЧ (например при не изплащана на поет ангажимент от ДЧ може да не може да гласуват.

Предвижда се също така преобладаващата част от финансирането да се предоставя след открити покани за представяне на предложения и на покани за представяне на оферти. Крайното решение за отпускане на финансова подкрепа ще се взима от Експертният център.

II.1.1.4 Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета от 14 декември 2022 година относно мерки за високо общо ниво на киберсигурност в Съюза, за изменение на Регламент (ЕС) № 910/2014 и Директива (ЕС) 2018/1972 и за отмяна на Директива (ЕС) 2016/1148 (Директива МИС 2)

Директивата за мрежова и информационна сигурност (ДМИС 2) е общоевропейското законодателство в областта на киберсигурността. В него се предвиждат правни мерки за високо ниво на киберсигурност в ЕС.

С нея се актуализират съществуващите преди това правила с Директива (ЕС) 2016/1148 за повишаване нивото на мрежовата и информационната сигурност (МИС) в Съюза.

Основни акценти

Предвидените мерки в ДМИС 2 са насочени към подобряване на киберсигурността в Съюза с цел създаване на условия за по-добро функциониране на вътрешния пазар.

За тази цел с ДМИС 2 се установяват:

1. задължения за ДЧ да приемат национални стратегии за киберсигурност, да определят или създадат национални компетентни органи, органи за управление на киберкризи, единни звена за контакт по въпросите на киберсигурността (единни звена за контакт) и екипи за реагиране при инциденти с компютърната сигурност (ЕРИКС), мерки за управление на риска в областта на киберсигурността и задължения за докладване за субекти, установени като критични съгласно Директива(ЕС) 2022/2557, правила и задължения относно обмена на информация за киберсигурността, задължения за надзор и правоприлагане за държавите членки и др.

2. ДМИС 2 се прилага за публични или частни субекти които покриват или надхвърлят критериите за средни предприятия от общо 18 сектора в националните стопанства. В обхвата на прилагането са предвидени и изключения отнасящи се до субекти независимо от тяхната големина. Директивата не се прилага за публични органи осъществяващи дейности в областта на националната сигурност.

ДМИС 2, разделя субекти на две категории – съществени и важни.

1. Първата категория субекти - съществени субекти са преди всичко от сектори с висока степен на критичност. Като такива сектори се определени - енергетика,всички видове транспорт, банков сектор и инфраструктури на финансовия пазар, здравеопазване, производство на фармацевтични продукти, и питейна и отпадъчна вода; цифровата инфраструктура и не на последно място публичната администрация.

2. Втората категория субекти – важни субекти са с по-ниска степен на критичност сектори. Някои от тези сектори са: пощенски и куриерски услуги; управление на отпадъците; химикали и храни; производство на медицински изделия, компютри и електроника, машини и оборудване, моторни превозни средства, доставчици на цифрови услуги (онлайн места за търговия, онлайн търсачки и платформи на услуги за социални мрежи) и др.

Всяко предприятие от посочените сектори с повече от 50 служители или с годишен оборот над 10 млн. евро попада в обхвата.

По този начин се въвеждат изисквания за всеки един от тези субекти да прилага в дейностите си изискванията на настоящата ДМИС. Следва да се имат предвид и субектите които попадат в обхвата, независимо от броя на заетите в тях служители.

Национална стратегия за киберсигурност

ДЧ следва да приемат национална стратегия за киберсигурност, коя предвижда стратегическите цели, необходимите ресурси за постигане на тези цели и подходящи мерки на политиката, както и подходящи регулаторни мерки. Тя включва цели и приоритети и рамка за постигането им, заинтересовани страни и сътрудничество, установяване на относими активи и оценка на риска за тях, мерки за действие при управление на инциденти; мерки за координация; план с мерки за повишаване осведомеността на гражданите и др. Посочени са и десет направления, в които следва да се разработят политики, които да са част от Стратегията.

Органи по киберсигурност

Стратегията изисква да се създадат – Национални компетентни органи (един или няколко); национално единно звено за контакти, Екипи за реагиране при инциденти с компютърната сигурност и органи за управление на киберкризи. За всеки един от тях са посочени задачите, които следва да решава, както и изискванията на които следва да отговаря.

Изрично изискване на ДМИС 2 е ДЧ да гарантират, че тези органи разполагат с адекватни ресурси за изпълнение на възложените им задачи по ефективен и ефикасен начин.

Национална рамка за управление на киберкризи - освен създаване/определяне на орган ДМИС 2 се поставя изискване ДЧ да идентифицират и подготвят способности, активи и процедури за реакция при киберкризи. Изисква се също така и изготвянето на Национален план за управление на киберкризи.

Координирано оповестяване на уязвимости – предвиден е ред за идентифициране на уязвимости и ред за уведомяване на заинтересованите страни за тези уязвимости.

Сътрудничество на национално ниво – В ДМИС 2 са предвидени изисквания за сътрудничество между различните органи по киберсигурност, включително и императивното такова, за докладване при значителни инциденти.

Сътрудничество на равнището на Съюза – извършва се основно в рамките на специално създадени за целта структури: - на Стратегическо/политическо ниво посредством Групата за сътрудничество; на оперативно ниво чрез Европейска мрежа за връзка на организациите при киберкризи, на тактическо ниво в мрежата на европейските национални Екипи за реагиране при инциденти с компютърната сигурност. За всяка една от тези структури на европейско ниво, в ДМИС 2 се съдържат цели, ред за работа, задачи за изпълнение и др.

Партньорски проверки

ДМИС 2 предвижда механизъм за партньорски проверки

Мерки за управление на риска в областта на киберсигурността

Едно от най-важните изисквания на ДМИС 2, е ДЧ да гарантират, че съществените и важните субекти предприемат подходящи и пропорционални технически, оперативни и организационни мерки за управление на рисковете за МИС на субектите при предоставяне на своите услуги, както и за предотвратяване или свеждане до минимум на въздействието на инцидентите върху получателите на услугите им и върху други услуги. При това следва да се вземат отчитат последните достижения в тази област и да се имат предвид приложимите европейски и международни стандарти за киберсигурност. Мерките, следва, се основават на подход, обхващащ всички опасности, който има за цел да осигури МИС от инциденти, и включват поне следното: Политики за анализ на риска и за МИС; действия при инцидент; непрекъснатост на основната дейност; сигурност на веригата за доставка; сигурност при придобиването на мрежи и информационни системи; политики и процедури за оценяване на ефективността на мерките за управление на риска в областта на киберсигурността; основни киберхигиенни практики и обучение в областта на киберсигурността; политики и процедури относно използването на криптография; сигурност на човешките ресурси, политики за контрол на достъпа и управление на активи и др.; изисква се субектите в случаи на необходимост да предприемат незабавно подходящи и пропорционални коригиращи мерки.

Задължения за докладване – предвидени са изискванията за докладване – кой, кога, за какво и на кого докладва.

Надзор и правоприлагане. - от ДЧ се изисква да гарантират, че техните компетентни органи ефективно осъществяват надзор и предприемат мерки, необходими за осигуряване на спазването на настоящата директива. Регламентират се и видовете проверки, одити, за киберсигурността на субектите, реда и последователността за извършването им, а така също и изискванията за правомощия на органите осъществяващи надзор. Съществените субекти в подлежат на всеобхватен предварителен и последващ контрол Важни субекти ще подлежат единствено на последващ надзор.

За неспазване на изискванията заложени в Директивата се предвиждат значително високи финансови санкции, съизмерими с тези по Регламента за защита на личните данни (GDPR), например.

Санкциите за съществените субекти ще достигат 10 млн. евро, или 2% от техния световен годишен оборот;

Санкциите за важните субекти ще достигат 7 млн. евро или 1.4% от световния им годишен оборот.

ДЧ ще могат по тяхна преценка да въведат и по-висок максимален размер. Наред с това, към органите е предвидено изискване да имат и други съществени правомощия: да спрат/преустановят действието временно или да изискат временно преустановяване на действието на удостоверение или разрешение на субектите; да забранят временно на ръководителите/управителите да изпълняват задълженията си; да назначат временно длъжностно лице по надзор, който да следи за спазването на изискванията от страна на субектите.

Специално внимание в ДМИС 2 е обърнато на отговорностите на ДЧ по отношение на членовете на ръководните/управителните органи на основни и важни субекти. ръководните/управителните органи / на съществени и важни субекти ще носят и лична отговорност за неспазване на ДМИС 2. Това е новост (в България съществува към настоящия момент и е регламентирано в Закона за киберсигурност) и е изрично предвидена като инструмент, който да гарантира, че ръководните/управителни органи в компаниите ще предприемат необходимите стъпки и действия да прилагат надлежно всички нови мерки. ДЧ гарантират, че е възможно членовете на тези органи да бъдат подвеждани под отговорност за неизпълнението на своите задължения да осигурят спазването на настоящата директива. За тази цел от тях ще се изисква да преминават специални обучения, а

субектите ще бъдат насърчавани да предлагат редовно подобни обучения на своите служители.

II.1.1.5 Регламент (ЕС) 2022/2554 на Европейския парламент и на Съвета от 14 декември 2022 година относно оперативната устойчивост на цифровите технологии във финансовия сектор (DORA)

Регламентът е в сила от 16 януари 2023 г. и се прилага от 17 януари 2025 г. DORA е подкрепен от Директива за изменение (ЕС) 2022/2556, която привежда в съответствие някои настоящи директиви на ЕС за финансови услуги.

Основни акценти

1. Целта на DORA - е предотвратяване и/или смекчаване на киберзаплахи във финансовата сфера. За изпълнение на целта, DORA определя единни изисквания относно сигурността на мрежовите и информационните системи, които са в основата на бизнес процеса на финансовите субекти. Изисквания приложими към субектите на DORA са: управление на риска и ИКТ; докладване за големи киберинциденти; цифрово тестване на оперативната устойчивост; споделяне на информация; приемане на правила за провеждане на надзор и др.

2. Обхват –Регламентът обхваща почти всички субекти от следните 21 категории финансови институции (финансови субекти) - кредитни институции; платежни институции; доставчици на услуги за информация за сметки; институции за електронни пари; инвестиционни посредници доставчици на услуги за крипто активи и емитенти на токени; централни депозити на ценни книжа; места за търговия; търговски хранилища; мениджъри на алтернативни инвестиционни фондове; управляващи дружества; застрахователни и презастрахователни предприятия; застрахователни посредници; агенции за кредитен рейтинг; доставчици на услуги за групово финансиране; хранилища за секюритизация; доставчици на ИКТ услуги от трети страни.

<u>Основни акценти</u>

Управление на риска в ИКТ

1.Управление и организация

Финансовите субекти трябва да разполагат с рамка за вътрешно управление и контрол, която осигурява ефективно управление на риска за ИКТ; управителния орган на финансовия субект отговаря за изпълнение на Рамката;

носи крайна отговорност за управление на риска; за въвеждането на политики за наличност, автентичност, цялост и поверителност; определя ясни роли и отговорности за всички функции и др.; определят член на ръководството на субекта които контролира риска с доставчици на ИКТ.

2. Рамка за управление на риска

Рамката трябва да включва най-малко стратегии, политики, процедури, протоколи, необходими за защита на ИКТ, с чието прилагане минимизират риска; финансовите субекти осигуряват разделение на функциите по отношение на ИКТ – управление на риска, контрол и вътрешен одит. Рамката се преглежда и актуализира минимум един път годишно и др.

3.Процес за управление на инциденти, свързани с ИКТ

От финансовите субекти се изисква да определят, установят и прилагат процес за управление на инциденти; да класифицират инцидентите в съответствие с посочените критерии; докладват за големи инциденти на съответния компетентен орган

4. *Тестване на цифровата оперативна устойчивост*

Финансовите субекти се задължават да създават, поддържат и преразглеждат програма за изпитване на цифровата оперативна устойчивост,

управление на риска от трета страна. – като част от риска предвиден в тяхната рамка за управление на риска.

5.Наказателни санкции – ДЧ могат да не определят правила за административни санкции или коригиращи мерки за нарушения и операции.

II.1.1.6 Закон за киберустойчивостта (в процес на приемане)

С предложението за Регламент относно изискванията за киберсигурност за продукти с цифрови елементи, (Законодателен акт за киберустойчивостта), укрепва правилата за киберсигурност, с цел да се създадат условия за гарантиране на по-сигурни хардуерни и софтуерни продукти.

В предложението за Регламент са набелязани две основни цели, и четири конкретни цели насочени към осигуряване на правилното функциониране на вътрешния пазар:

1. основна цел - създаване на условия за разработването на сигурни продукти с цифрови елементи.

2. конкретни цели - гарантиране, че производителите подобряват сигурността на продуктите с цифрови елементи от началото до края на жизнения цикъл; осигуряване на съгласувана рамка за киберсигурност; повишаване на прозрачността на свързаните със сигурността свойства на продуктите с цифрови елементи и да се даде възможност на предприятията и потребителите да използват продуктите с цифрови елементи по сигурен начин.

Предложението е в етап на разглеждане на различни нива. Към настоящия момент редица текстове в него са спорни и силно критикувани. По време на проведеното обществено обсъждане от ЕК, над 130 професионални асоциации и сдружения са изразили отрицателно становище.

II.1.1.7 Законодателен акт за солидарност в киберпространството (в процес на приемане, приет от ЕК и от Съвета на ЕС, предстои приемане от Европейския парламент)

С цел повишаване готовността за реакция при киберзаплахи, Европейската комисия предложи Акт на ЕС за солидарност в киберпространството.

Предложението включва създаването на европейски щит за киберсигурност и на широкообхватен механизъм за управление на извънредни ситуации в киберпространството.

Основните три действия на ниво ЕС предвидени в Регламента са:

1. Създаване на Система за оповестяване за киберзаплахи и киберинциденти.

2. Създаване на Европейски механизъм за действия при извънредни ситуации в киберсигурността.

3. Създаване на Европейски механизъм за преглед и анализ на широкомащабни киберинциденти в Съюза.

С Предложението се предвиждано укрепване способностите на ЕС за откриване, подготовка и реагиране на значителни и широкомащабни киберзаплахи и кибератаки. Европейският щит за киберсигурност, ще се изгради на базата на взаимосвързани оперативни центрове за сигурност, в целия ЕС. За оперативните центрове се предвижда изграждането на многонационална платформа с финансови средства по програма „Цифрова Европа“ и национално съфинансиране.

II.1.1.8 Други

II.**1.1.8.1 Препоръка (ЕС) 2017/1584 на Комисията от 13 септември 2017 година, относно координирана реакция на мащабни киберинциденти и кризи.**

С Препоръката се предвижда:

1 Институциите на ЕС съвместно с ДЧ да създадат Механизъм на ЕС за реакция при киберкризи.

2. Механизмът на ЕС за реакция при киберкризи определя участниците от ДЧ и от институциите на ЕС в управлението им на различни нива на управление - техническо, оперативно и стратегическо/политическо.

Предвижда се да бъдат разработени стандартни оперативни процедури за управление на киберкризи. От ДЧ се изисква да осигурят наличието на структури за обмен на информация между участниците в управлението на киберкризи. Следва да се планират, подготвят и провеждат регулярни учения с участниците в управлението на киберкризи на всички нива.

Към Препоръката е разработена и приложена Концепция за координирана реакция при трансгранични киберинциденти и при киберкризи.

При разработване на Концепцията са взети предвид като ръководни принципи (пропорционалност, субсидиарност, взаимно допълване и поверителност на информацията).

Предложението е съобразено и с факта че киберинцидентите могат да бъдат в основата на по-широкомащабни кризи или да бъдат част от такива кризи, засягащи и други сектори. Поради това дейностите по управление на киберкризи са релевантни на съществуващите механизми и процедури за управление на кризи на ниво ЕС и на ниво ДЧ.

II.1.1.8.2 Киберпрестъпност

Според различни статистики над един милион души ежедневно стават жертва на киберпрестъпления. Финансовите щети растат главоломно. ДЧ и органите, институциите и агенциите на ЕС не правят изключения от тези тенденции. Специализирани структури на Европейската комисия наблюдават и в случаи на необходимост предприемат действия за актуализиране правото на ЕС в областта на киберпрестъпността. и подпомага укрепването на капацитета на

правоприлагащите органи. Комисията също така работи съвместно по различни направления с Европейския център за борба с киберпрестъпността в Европол.

II.1.1.8.3 Киберотбрана

Във връзка с влошаващата се и усложняваща се среда за сигурност след агресията на Русия, Комисията съвместно с Върховния представител публикуваха съвместно съобщение относно политиката на ЕС за киберотбрана. В областта на киберотбрана ЕС формира дейностите си около четири основни направления – съвместни действия за по-силна киберотбрана подсигуряване по отношение на киберсигурността на отбранителната екосистема; инвестиране в изграждане на способности по киберотбрана; ЕС, като партньор при справяне с киберпредизвикателства.

ЕС призовава ДЧ за увеличаване на инвестициите в широк спектър способности за киберотбрана. Съюзът също така ще предприема действия за по-добра координация и по-тясно сътрудничество между военните и гражданските структури по киберсигурност в Съюза. ЕС също така предвижда засилване на сътрудничеството с гражданското общество, частния сектор за пълноценно управление на киберкризи.

В рамките на ЕС в сътрудничеството в областта на киберотбраната са ангажирани Европейската комисия, Европейската служба за външна дейност, Европейската агенция по отбрана, както и ENISA и Агенцията на Европейския съюз за сътрудничество в областта на правоприлагането (Европол).

II.1.1.8.4 Кибердипломация

Водеща тенденция в свързана с киберсигурността е нарастване ролята на кибердипломацията, като един от инструментите за защита на Съюза от кибератаки идващи от държави извън неговите граници. Във връзка с това ЕС в Стратегията си за киберсигурност включи кибердипломацията като нов стълб (четвърти) на киберсигурността. Комисията работи в тясно сътрудничество с Европейската служба за външна дейност както при разработването на различни правно-нормативни документи на европейско ниво, така и при прилагането на киберинструментариум в случаи на злонамерени кибердействия в европейското киберпространство. Киберинструментариумът включва дипломатическо

сътрудничество и диалог, превантивни мерки срещу кибератаки и санкции срещу лицата, участващи в кибератаки, застрашаващи ЕС.

II.1.1.8.5 Изкуствения интелект в Европа – гарантиране на киберсигурността

БЯЛА КНИГА за изкуствения интелект в Европа в търсене на високи постижения и атмосфера на доверие; Съобщение на Комисията до Европейския парламент, Съвета, Икономическия и социален комитет и Комитета на регионите – изкуствен интелект за Европа (Европейска Стратегия).

Стратегията и Бялата книга са ключови документи относно Изкуствения интелект в ЕС и необходимостта той да гарантира киберсигурността на потребителите му.

Основни акценти

В документите се подчертават, че сложната благоприятстваща екосистема и функцията за автономно вземане на решения, присъщи на Изкуствения интелект(ИИ), изисква да се обърне внимание на устойчивостта на някои установени правила по въпросите на киберсигурността. ИИ носи много ползи, сред които е повишаването на сигурността на някои ИКТ продукти, ИКТ процеси и ИКТ услуги, но той може да донесе и вреди.

Като пример са посочени вероятността усъвършенстваните роботи и продукти за „интернет на нещата (IoT), задвижвани от ИИ, могат да действат по начини, които не са предвидени по времето, когато системата е пусната в експлоатация за първи път. Като се имат предвид разнообразните приложения на ИИ, налага се преразглеждане както на хоризонталните, така и на секторните правила.

Рамката за сигурност се отнася до предвидената употреба и (зло)употреба на продукти при пускането им на пазара. По тази причина възниква необходимост от разработването на множество от стандарти в областта на устройствата, използващи ИИ по отношение на киберсигурността, които постоянно се адаптират, за да съответстват на развитието на технологиите.

Използването на ИИ в ИКТ продукти, ИКТ процеси и ИКТ услуги може да доведе до рискове, които понастоящем не са изрично посочени в законодателството на ЕС. Те могат да са свързани с киберзаплахи, свързани с нови приложения на ИИ, например в домакинските уреди), рискове които произтичат

от загуба на връзка с интернет и т.н. Тези рискове могат да са налице в момента на пускане на продуктите на пазара или да възникнат.

ИИ носи много ползи, сред които е повишаването на сигурността на някои ИКТ продукти, ИКТ процеси и ИКТ услуги, но той може да донесе и вреди.

II.1.1.8.6 Инструментариум на ЕС за сигурност на 5G мобилни електронни съобщителни мрежи

Инструментариумът представлява набор от стабилни и всеобхватни мерки за координиран подход на ЕС за гарантиране сигурността на 5G мрежите.

Новата технология в мобилните електронни съобщителни мрежи 5G се очаква да се превърне в нова инфраструктура за свързаност, чрез която ще се предоставят нови продукти и услуги във всички сфери на обществото. С оглед на това че 5G мрежите са бъдещият гръбнак на все по-цифровизирани икономики и общества. Те ще са релативни с милиарди свързани системи, милиарди свързани предмети и системи, включително и такива в чувствителни и критични инфраструктури. Поради това киберсигурността на 5G мрежите придобива изключително важно значение.

Във връзка с това, ЕС извърши Оценка на риска - Координирана оценка на ЕС на риска за сигурността на 5G мрежата, която идентифицира девет основни риска, групирани в пет сценария за риска.

Мерките в Инструментариума са насочени към смекчаване на рисковете с цел повишаване на увереността, че в ЕС функционират устойчиви 5G мрежи. В него се определят подробни планове за смекчаване за всеки от установените рискове и се препоръчва набор от ключови стратегически и технически мерки, които следва да бъдат предприети от всички ДЧ и/или от Комисията. Инструментариума съдържа и Примерен план за смекчаване на риска.

II.1.1.8.7 Съобщение на Комисията до Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите Гарантиране на свободни и честни европейски избори (Към настоящия момент документа са актуализира)

Настоящето съобщение е публикувано по повод провеждане на Изборите за Европейски парламент през май 2019 г.

В него под формата на Компендиум са отправени най-важните мерки за осигуряване високо ниво на киберсигурност по време на избори – Предоставяне

на конкретни насоки по отношение на обработването на лични данни при избори; Препоръчване на най-добри практики за преодоляване на рисковете от дезинформация и кибератаки и насърчаване на онлайн прозрачността и отчетността на изборния процес на ЕС както и засилване на сътрудничеството между компетентните органи и създаване на инструменти, които да им позволят да се намесват и при необходимост да въвеждат санкции за запазване на целостта на изборния процес; справяне със ситуации, при които политическите партии или свързаните с тях фондации се ползват от практики, нарушаващи правилата за защита на данните, с цел умишлено оказване на влияние или опит за оказване на влияние върху резултата от европейските избори.

В новия документ който е в процес на разработване са посочени – възможни видове атаки, възможното им въздействие; таргетирани за избори, инициативи за сигурни избори; сътрудничество и обмен на релевантна информация; осведоменост; управление на риска; учения и тренировки; добри практики.

II.1.1.8.8 Европейска рамка за умения в киберсигурността

В Рамката са разработени подробни ролеви профили за 12 най-често срещани специалисти в сферата на киберсигурността. Разработването на профилите е продиктувано от необходимостта от тясно специализирани и високоподготвени специалисти по киберсигурност в рамките на Съюза.

II.2. Перспективи пред киберустойчивостта в България

Преглед на съществуващата в страната правно-нормативна уредба в сферата на киберсигурността

Прегледа е извършен с фокус върху наличието (степента на транспониране на европейските изисквания за киберсигурност)

II.2.1 Актуализирана национална стратегия за киберсигурност „Киберустойчива България 2023“

С Решение №301 от 02 април 2021 година, на Министерския съвет на Р България е приета Актуализирана национална стратегия за киберсигурност „Киберустойчива България 2023“.

Необходимостта от разработването и поизтича от изтеклия срок на приложимост на предходната ата стратегия за киберсигурност „Киберустойчива България - 2020“, както и от ускореното развитие на цифровата трансформация. Краткосрочният и тригодишен срок на актуалност от своя страна е обусловен от

очакваното приемане на основни нормативни документи на европейско ниво – ДМИС 2, Директива за устойчивост на критични субекти, Регламент за оперативна цифрова устойчивост.

Стратегията е съобразена с настъпилите промени в киберпространството и новоприети законодателни документи в страната за периода 2016-2020 г.(най-вече Закона за киберсигурност), както и с настъпилите промени в киберпространството. При разработването и е взета предвид и Националната програма за развитие България 2030.

Предмет на стратегията към момента на нейното изготвяне са редица ключови и актуални въпроси за киберустойчивостта в страната. За достигане на киберустойчивост, като най-високо ниво на зрялост, са необходими систематични, планирани и координирани действия на всички заинтересовани страни, ясно определени и изцяло реализирани мерки планирани за целта.

Разработени са всеобхватни стратегически дейности с изпълнението на които в страната ще се създадат условия за постигане на киберустойчиво състояние.

Основни акценти

– стратегическа цел, принципи, приоритети, и приоритетни насоки за действие, установяване и развитие на националната система за киберсигурност, като част от системата за защита на националната сигурност политики, стратегии и планове - стратегическо ниво; оперативни координации; национална система за управление при киберкризи повишаване на ролята и отговорностите на държавните структури и на заинтересованите страни; МИС – фундамент на киберсигурността, изграждане на среда за сътрудничество и партньорство налагане на минимално общо ниво на МИС на ниво организация роли и отговорности по отношение на МИС; интегриране на Националната система за киберсигурност в европейските структури и инициативи в областта на МИС; ангажиране на частния сектор в повишаване нивото на МИС; провеждане на информационни кампании за киберсигурност и киберхигиена; повишаване на уменията и професионалните компетентностите на експертите по МИС; установяване на ефективни механизми за споделяне на информация и ангажираност на всички заинтересовани.

Наред с това е обърнато внимание и на други важни аспекти на киберустойчивостта - използване на обща комуникационна стратегия за

повишаване на осведомеността, осигуряване на достъп до устойчив достъп до интернет, актуализиране на правната рамка, фокус върху изследванията и иновациите в киберсигурността, необходими усилия за подобряване образование и обучение, международно сътрудничество, включително кибердипломация, взаимодействие на техническо, оперативно и стратегическо ниво реализиране, контрол и актуализация.

При актуализирането на Стратегията са взети предвид възможностите, за които се предоставят за финансиране по Механизма за възстановяване и устойчивост на ЕС, както и възможностите за предоставяне на средства европейските фондове и оперативни програми през следващия програмен период 2021-2027 г.

За изпълнение на целите и набелязаните мерки на Актуализираната стратегия е предвидено към нея да се разработи Пътна карта, която следва да бъде приета с акт на Министерския съвет.

Мониторинг и оценка на изпълнението и периодична актуализация на Стратегията и Пътната карта е предвидено да се осъществява от Съвета по киберсигурност (по смисъла на закона за киберсигурност).

В хода на изготвянето на настоящия анализ не бяха установени наличието на такава Пътна карта, както и за осъществяван мониторинг и оценка на степента на изпълнение на Стратегията, от страна на Съвета по киберсигурност.

II.2.2 Зкон за киберсигурност

С приетия на 31.10.2018 г. Закон за киберсигурност 5, в националното ни законодателство се транспонират изискванията на Директива (ЕС) 2016/1148 на Европейския парламент и на Съюза относно мерки за високо общо ниво на сигурност на мрежовите и информационните системи на Съюза.

Законът е първото специализирано законодателство в сферата на киберсигурността в страната.

Законът за киберсигурност урежда организацията, управлението и контрола на киберсигурността, предприемането на необходимите мерки за постигане високо общо ниво на МИС, както правомощията и функциите от системата за управление на киберсигурността. В обхвата на Закона са включени широк кръг субекти, като административните органи, лицата осъществяващи публични функции, организациите предоставящи обществени услуги и ново

въдените категории - оператори на съществени услуги и доставчици на цифрови услуги.

Секторите от националното стопанство, в които са определени операторите на съществен и услуги са – енергетика, транспорт, банково дело, инфраструктури на финансовия пазар, здравеопазване, доставка и снабдяване с питейна вода, цифрова инфраструктура. В Закона са дефинирани условията, за да бъде определен оператор от горепосочените сектори, като оператор на съществени услуги дали предоставяната услуга от него е съществена – услугата да е от основно значение за поддържането на осолено важни обществени, или стопански дейности; услугата да зависи от функционирането на мрежи и информационни системи евентуален инцидент би имал значително увреждащо въздействие върху услугата.

Не попадат в обхвата на Закона така наречените „силови“ ведомства.

Законът съдържа управленска рамка за киберсигурност.

Посочени са изискванията за създаване на Национална стратегия за киберсигурност, както и за това на какви условия трябва да отговаря. В нея е предвидено, че системата за киберсигурност се управлява и организира от Министерския съвет (МС), който определя националната политика за киберсигурност и постигане на киберустойчивост, която се реализира от различни държавни институции. В дейността си, МС се подпомага от Съвет по киберсигурност – консултативен, нещатен, постоянен орган, чиито състав и функции са определени от Закона.

Въвежда се и институцията национален координатор по киберсигурност с ясно определени функции и отговорности.

Управленската рамка за киберсигурност е структурирана по модел „Децентрализиран подход“ – с допълнително определени с Решение на МС, административни органи към които се създават, национални компетентни органи и екипи за реагиране при инциденти с компютърната сигурност. Този подход се характеризира със следните принципи – субсидиарност; силно сътрудничество между публичните органи, секторно законодателство и е един от съществуващите подходи в практиката на част от ДЧ.

Останалите органи за управление на киберсигурността предвидени в Закона са – министъра на електронното управление, министъра на вътрешните работи министъра на отбраната, председателя на Държавна агенция „Национална

сигурност“, като за всеки от тях са посочени неговите отговорности и функции. На министъра на електронното управление е възложено да осъществява контрол за спазване на изискванията за мрежова и информационна сигурност от административните органи (чл.12, т.5). На него са делегирани и правомощия за даване на методически указания и координиране на изпълнението на политиките за МИС.

Със Закона се създават специализирани ключови структури за изпълнение на целите му, като – национални компетентни органи, национално единно звено за контакти, национален и секторни екипи за реагиране при инциденти с компютърната сигурност. За тези органи, Законът съдържа изисквания, на които те следва да отговарят, както и функциите, които следва да изпълняват.

Специално внимание е отделено на въпросите по сътрудничество и координация. На стратегическо ниво тези дейности се осъществяват от Съвета по киберсигурност. Координацията на дейностите по изграждане на междуведомствена координационно-организационна мрежа и на Национален киберситуационен център е възложена на Министерство на електронното управление. В текстовете на Закона за киберсигурност относно Системата за киберсигурност е предвидено, че отговорността за неутрализиране, защита реакция при киберзаплахи и киберинциденти се възлага на четири ведомства. В рамките на отделения му бюджет, всяко ведомство изгражда способности за изпълнение на поставените му задачи, участва в процесите на формулиране на политики за киберсигурност и отговаря за съответните оперативни дейности. Практическата им реализация изисква взимането на съответстващи организационни и ресурсни решения. Изграждането на Системата за киберсигурност през този период (2018-10.02.2024 г.) се извършва в условията на ограничени човешки и финансови ресурси. С така съществуващият модел се възлагат отговорности на отделни ведомства по някои от областите на кибер сигурността (например, противодействие на кибер престъпността – ГДБОП, защита на обекти и дейности със стратегическо значение за националната сигурност – ДАНС, защита на информационната инфраструктура на публичната администрация – ДАЕУ, службите за сигурност – защита на собствените информационни инфраструктури и противодействие на кибер шпионаж и др.). За координация и обмен на информация на при възникване на инциденти, или при

извършване на компютърно престъпление на междуведомствено ниво се създават звена за контакт в съответните ведомства. Сътрудничеството и координацията се осъществяват посредством национална координационно-организационна мрежа и национален киберситуационен център, които следва да бъдат изградени.

Съществена част от разпоредбите на Закона се отнасят да задължения на всяка една от петте категории субекти по отношение на изискванията за сигурност и своевременното уведомяване за инциденти.

В тази част, на Закона е подчертана личната отговорност на всеки един административен орган или ръководител/управител на останалите субекти за спазване изискванията му.

Законът съдържа и други разпоредби, като - отговорности за планиране, подготовка и провеждане на национални киберучени и участие в международни такива (Cyber Europa, Cyber Coalition и др.).доброволно уведомяване за инциденти; юрисдикция и териториалност; административно-наказателни разпоредби.

Законът има важен принос за таксономията свързана с нормативно дефиниране на най-използваните определения в сферата на киберсигурността.

Съдържащите се в Закона изисквания надхвърлят тези предвидени в Директива (ЕС) 2016/1148 за повишаване нивото на мрежовата и информационната сигурност в Съюза (ДМИС) и другите европейски документи са сферата на киберсигурността съществуващи към началото на 2018 г. Така например в него са включени като субекти административните органи, лицата осъществяващи публични функции и организациите предоставящи обществени услуги; предвидени са задължения към предприятията, предоставящи обществени електронни съобщителни мрежи или услуги да съдействат на Националния екип за реагиране при инциденти с компютърната сигурност за отстраняване на установени от него инциденти техните мрежи и/или услуги.

До 24.10.2024 г. следва да се изготви и приеме Закон за изменение и допълнение на Закона за киберсигурност, който да транспонира в националното ни законодателство комплекта документи по КС, приети от ЕС в периода от 2016 г, до момента на разработването му.

II.2.3 Национална развитие на България 2030

Програмата е рамков стратегически документ, определящ визията и общите цели на политиките за развитие във всички сектори на държавното управление, включително техните териториални измерения.

Програмата включва детайлизирани стратегии по приоритетите, индикативна финансова рамка, предварителна оценка на въздействието върху основни макроикономически индикатори от изпълнението на заложените интервенции, както и механизъм за наблюдение и контрол на изпълнението на стратегическия документ. В документа са посочени областите на въздействие в които е предвидено до 2030 г., да има целеви инвестиции.

В приоритет 10 - „Институционална рамка“, като област на въздействие в под приоритет 10.3, Електронно управление“, е посочена Мрежовата и информационната сигурност.

В Програмата е отбелязано, че Мрежовата и информационната сигурност е важен фактор за доверието на потребителите в електронните услуги. Сигурността на широкото използване на продукти и услуги, базирани на данни ще зависи от прилагането на най-високи стандарти за киберсигурност.

За целта са предвидени институционализирана единна система за мониторинг на общото състояние на киберпространството, за превенция и възстановяване от киберинциденти и за анализ и противодействие на киберзаплахите.

За постигането на тези цели са планирани финансови средства в размер на 550 млн. лв.

II.2.4 Други документи

1. Наредба за минималните изисквания за мрежова и информационна сигурност.

В допълнение към Закона и в съответствие с чл.3, ал.2 от него е разработена Наредба за минималните изисквания за МИС. Наредбата е разработена в съответствие с изискванията на съществуващите стандарти за сигурност на информацията от серията ISO/IEC -27000.

С Наредбата се уреждат – изисквания към минималните и препоръчителните марки за МИС, както и правилата за извършване на проверки одит за съответствие с изискванията и.

Регламентирано е, че прилаганите мерки следва да са пропорционални, технически, технологични и организационни. Насочеността на Наредбата е към спазване на съответните законови, подзаконови и договорни задължения по отношение на МИС, оптимизирано използване на наличните ресурси, както и периодични вътрешни проверки на системата с цел непрекъснато усъвършенстване.

В рамките на проект по ОП „Добро управление за Проект „Повишаване на общото ниво на мрежова и информационна сигурност в общински администрации“ е разработена Методика за оценка на риска и за одит на общинско ниво. Извършен е и Анализ на резултатите от Изследване и мониторинг на ефективното прилагане на Наредбата за минималните изисквания за мрежова и информационна сигурност от 16 общини първа, втора и трета категория.

Анализът е изготвен на база извършена самооценка от общините въз основа на специално създаден за целта въпросник. дава аналитична информация в каква степен са приложени изискванията на Наредбата. Методиката е с насоченост подпомагане на общините при извършване на оценка на риска и при извършването на одит за степента на съответствие на състоянието на мрежовата и информационната сигурност и изискванията на Наредбата.

2. Закон за електронните съобщения

Текстове, относими към киберсигурността съдържа и Закона за електронните съобщения. Към предприятията, предоставящи електронни съобщителни мрежи и/или услуги има изисквания да предприемат пропорционални технически и организационни мерки за управление на риска за МИС; Комисията за регулиране на съобщенията да приеме правила за мрежова и информационна сигурност. Регламентиран е и реда за уведомяване при инциденти с МИС и регулярното информиране на ENISA и на националния екип за реагиране при инцидент; случаите за извършване на одит за състоянието на мрежовата и информационната сигурност в предприятията.

3. Законите за МВР, за ДАНС, електронния документ и електронния подпис също съдържат релевантни на темата за киберсигурността, текстове.

4. Релевантни Решения на Министерския съвет

Решение №192 от 09 април 2019 година за определяне на административни органи, към които се създават национални компетентни органи по МИС –сектор „Енергетика“ –Министерство на енергетиката; за сектори

„Транспорт“, „Цифрова инфраструктура“ и “Цифрови услуги“ – Министерство транспорта, информационните технологии и съобщенията; сектор „Здравеопазване“ – Министерство на здравеопазването; сектор „Доставка и снабдяване с питейна вода“ - Министерство на регионалното развитие и благоустройството.

С Решението е приета и Методика за определяне на операторите на съществени услуги по смисъла на Закона за киберсигурност.

Решение № 544 на Министерския съвет от 23 юли 2021 година определя Държавна агенция „Електронно управление“ за национален орган за сертифициране на киберсигурността.

Националният координационен център в сферата на киберсигурността е създаден с промяна в Устройствения правилник на Министерство на електронното управление, приет с ПМС№89 от 19.05.2022 г.

5. Програма за управление на Република България юни 2023г.- декември 2024 г.

В програмата, част „Електронно и ефективно управление са предвидени две дейности (от всичко 45 в тази част) с вързани с въпросите на киберсигурността. В Раздел „Законодателни мерки“ – Одобряване от Министерския съвет и внасяне в Народното събрание на Законопроект за изменение и допълнение на Закона за киберсигурност с предвиден краен срок, м. май 2024 г. В Раздел „Мерки в изпълнителната власт“ е предвидена мярката „Развитие на Национален компетентен орган по киберсертификация (правилното наименование съгласно Регламента е Национален орган за сертифициране на киберсигурността)“ с предвиден краен срок ноември 2024 г. С изпълнението на мярката се очаква да има Функциониращ национален компетентен орган за киберсертификация и въведени най-малко две схеми за сертификация.

/п/

Зорница Русинова

ПРЕДСЕДАТЕЛ НА ИКОНОМИЧЕСКИ И СОЦИАЛЕН СЪВЕТ

Приложение 1

Определения

За целите на настоящия Анализ са използвани следните определения:

„Киберустойчивост“ означава способността на субекта/организацията да се подготви, да реагира и да се възстанови след кибератака;

„Киберсигурност“ - Киберсигурността включва дейностите, необходими за защита от киберзаплахи на мрежите и информационните системи, на ползвателите на тези мрежи и системи и на други лица, засегнати от киберзаплахи.

„Мрежова и информационна сигурност“- Мрежова и информационна сигурност е способността на мрежите и информационните системи да се противопоставят на определено ниво на въздействия, засягащи отрицателно наличието, истинността, целостта или поверителността на съхранявани, пренасяни или обработвани данни или на свързаните с тях услуги, предлагани от тези мрежи и информационни системи или достъпни чрез тях".

„Киберзаплаха“ означава всяко потенциално обстоятелство, събитие или действие, което може да навреди, наруши или по друг начин да окаже неблагоприятно въздействие върху мрежите и информационните системи, ползвателите на такива мрежи и системи и други лица;

“Значителен инцидент“ - инцидентът се счита за значителен, ако:

а) е причинил или е в състояние да причини сериозно оперативно смущение в услугите или финансова загуба за засегнатия субект;

б) е засегнал или е в състояние да засегне други физически или юридически лица, причинявайки значителни материални или нематериални вреди.

„национална схема за сертифициране на киберсигурността“ означава цялостен набор от правила, технически изисквания, стандарти и процедури, разработени и приети от национален публичен орган и които се прилагат по отношение на сертифицирането или оценката на съответствието на ИКТ продукти, ИКТ услуги и ИКТ процеси, попадащи в обхвата на конкретната схема;

„европейски сертификат за киберсигурност“ означава издаден от съответния орган документ, удостоверяващ, че за даден ИКТ продукт, ИКТ услуга или ИКТ процес е извършена оценка за съответствие спрямо специфичните изисквания за сигурност, определени в дадена европейска схема за сертифициране на киберсигурността;

„ИКТ продукт“ означава елемент или група елементи на мрежа или на информационна система;

„ИКТ услуга“ означава услуга, състояща се в изцяло или главно в предаване, съхранение, извличане или обработка на информация посредством мрежи и информационни системи;

„ИКТ процес“ означава набор от дейности, извършвани с цел проектиране, разработване, предоставяне или поддържане на ИКТ продукт или ИКТ услуга;

„Фишинг“ означава вид социален инженеринг, при който нападателят изпраща целящо да подмами дадено лице да разкрие чувствителна информация на нападателя или да разположи зловреден софтуер в инфраструктурата на жертвата, например софтуер за откуп.

„Отказ на услуга (DDoS)“ означава атака не позволяваща на потребителите да получат достъп до дадена услуга, като претоварва нейните физически ресурси или мрежови връзки.

„Уеб-базирани атаки“ когато престъпниците използват уязвимости в кодирането, за да получат достъп до сървър или база данни.

„Рансъмуер“ - като вид атака, при която участниците в заплахата поемат контрола върху активите на целта и да изискват откуп в замяна на връщането на наличност на актива. Това е една от основните киберзаплахи през 2023 г., с няколко установени и анализирани киберинциденти.

„Зловреден софтуер (малуеър)“ Злонамереният софтуер, наричан още злонамерен код и злонамерена логика, е всеобхватен термин, използван за описание на всеки софтуер или фърмуер, предназначен за извършване на неразрешен процес, който ще има неблагоприятно въздействие върху поверителност, цялост или наличност на система.

„Социално инженерство“ - използва различни форми на манипулация, за да подмами жертвите да направят грешки или да предадат чувствителна или секретна информация. Потребителите могат да бъдат подмамени да отворят документи, файлове или имейли, за посещение на уебсайтове или за предоставяне на достъп до системи или услуги. атака: фишинг, spear-phishing, смишинг, примамка, претекст. Те могат да бъдат използвани и на по-късни етапи при инцидент или нарушение. такива примери са компрометиране на електронна поща (BEC), измама, представяне под чужда самоличност, фалшифициране.

„Заплахи срещу данни“- технически погледнато, заплахите срещу данните могат да бъдат класифицирани главно като нарушение на данните или изтичане на данни.

„Заплахи за наличност“ - наличността е цел на множество заплахи и атаки, които целят системата и наличност на данни и въпреки че не е нова заплаха, играе значителна роля в заплахата за киберсигурността. Атаките възникват, когато потребителите на система или услуга не могат да получат достъп до съответните данни, услуги или други ресурси. Това може да се постигне чрез изчерпване на услугата и нейните ресурси или претоварване на компоненти на мрежовата инфраструктура.

Приложение 2

Използвана литература

1.Закон за киберсигурност.

2.Наредба за минималните изисквания за мрежова и информационна сигурност - приета с РМС№186 от 26.07.2019 г., обн. ДВ бр.59 от 26.07.2019 г.

3.Актуализирана национална стратегия за киберсигурност „Киберустойчива България 2023“.

4. Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета от 17 април 2019 година относно ENISA (Агенцията на Европейския съюз за киберсигурност) и сертифицирането на киберсигурността на информационните и комуникационните технологии, както и за отмяна на Регламент (ЕС) № 526/2013 (Акт за киберсигурността).

5. Регламент (ЕС) 2021/887 на Европейския парламент и на Съвета от 20 май 2021 година за създаване на Европейски център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността и на мрежа от национални координационни центрове.

6. Регламент (ЕС) 2022/2554 на Европейския парламент и на Съвета от 14 декември 2022 година относно оперативната устойчивост на цифровите технологии във финансовия сектор и за изменение на регламенти (ЕО) № 1060/2009, (ЕС) № 648/2012, (ЕС) № 600/2014, (ЕС) № 909/2014 и (ЕС) 2016/1011

7. Регламент (ЕС) киберустойчивост (в процес на приемане).

8. Регламент (ЕС) за солидарност в киберпространството (в процес на приемане.

9. Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета от 14 декември 2022 година относно мерки за високо общо ниво на киберсигурност в Съюза, за изменение на Регламент (ЕС) № 910/2014 и Директива (ЕС) 2018/1972 и за отмяна на Директива (ЕС) 2016/1148 (Директива МИС 2).

10. Препоръка (ЕС) 2017/1584 на Комисията от 13 септември 2017 година, относно координирана реакция на мащабни киберинциденти и кризи.

11. Закон за електронните съобщения.

12. Закони за МВР, за ДАНС, за електронния документ и електронния подпис.

13. Национална програма за развитие БЪЛГАРИЯ 2030.

14.Програма на за управление на Република България юни 2023г.-декември.

15.Други национални и европейски документи релевантни на предмета на настоящия анализ.